



# INFORMATION AS A COMMODITY: NEW IMPERATIVES OF COMMERCIAL LAW

RAYMOND T. NIMMER\* AND PATRICIA ANN KRAUTHAUS\*\*

## INTRODUCTION

Modern information technology changes not only how commercial transactions occur, but also more fundamentally the subject matter of commerce itself.<sup>1</sup> It creates new products, which require re-examination of the definitions of property rights, liability, and contract terms relating to information rather than goods. The challenge posed to scholars and policymakers by these issues constitutes the new frontier of commercial law. This article discusses the emerging outlines of this challenge.

Modern information systems make possible the storage and transfer of vast amounts of factual material that can be accessed and analyzed through new technology. These systems enable the development of new information products and new approaches to handle these products. However, technology alone does not explain this growth of information as a commercial commodity. Indeed, treating the information age as merely a technological phenomenon would ignore significant social changes that concomitantly have greatly enhanced the value of information and the commercial need to control its use. Businesses, governments, and the general public today operate in a more information-dense environment than did their counterparts of a few decades ago. They increasingly rely on and consume information. Therefore, the task confronting commercial law is the formulation of principles that will facilitate the development of information transactions and products to meet this burgeoning demand, while preserving fundamental political and social values.

Part I of this article provides a format for discussing information products—how they differ among themselves and, more importantly, how they differ from other more conventional commercial products. The article then proceeds to examine two issues that form the core of an evolving legal structure to deal with information as a product. The first issue, discussed in Part II, defines the property rights that exist in information. The second issue, discussed in Part III, focuses on the qualitative assurances found in

---

Copyright © 1992 by Law and Contemporary Problems

\* Leonard Childs Professor of Law, University of Houston Law Center; counsel, Weil, Gotshal & Manges.

\*\* Attorney at Law, Houston, Texas.

1. See generally Peter F. Drucker, *Innovations and Entrepreneurship* (Harper & Row, 1985); Rebecca S. Eisenberg, *Proprietary Rights and the Norms of Science in Biotechnology Research*, 97 Yale L.J. 177 (1987) (discussing the conflicts patent law imposes on scientific research).

contracts for information products and how they differ from those found in transactions involving more conventional goods.

Our law defines as a positive social goal the promotion of a public domain of free, generally available factual information. As a result, it seeks to encourage the disclosure of information to the public and the creation of an environment conducive to the free use of the information thus disclosed. Countervailing principles, however, support a policy protecting confidential and secret information.

These competing values are accommodated by a distinction that is drawn between public disclosure and person-to-person uses of information. The law recognizes relatively limited property rights in generally disseminated information products, except with respect to patented technology, but it also implies only narrow assurances about their quality, thus arguably contributing to ready access and broad use. By way of contrast, for limited-distribution information products, the greater recognition of property rights is directly related to the effort to protect the private data. The law also creates a more robust structure of qualitative assurances for these products.

## I

### INFORMATION PRODUCTS

We must begin with an understanding of information products and how they differ from more conventional goods—the context in which modern commercial law developed. This is a relatively new field for commercial law inquiry.<sup>2</sup>

Information products differ from tangibles in both what constitutes value and what it means to sell, buy, or otherwise transfer the product.<sup>3</sup> Information does not exist in one place; rights in information thus cannot be defined by possession or a right to possess in the traditional sense. Theft of information does not resemble theft of a car and does not entail the same sort of overt acts. In many respects, the “property” that inheres in an information product is defined and perhaps even created by law, rather than merely reflected in legal principles.

---

2. Although trade in services and information has begun to exceed trade in goods as the defining characteristic of modern western industrial societies, the dominant method of thinking about political, social, and legal issues continues to focus on criteria and issues relevant to trade in, and manufacture of, goods. “This implicit ‘goods bias’ in our thinking makes it difficult both to perceive the real nature of our economy and to anticipate future changes in it which will affect the welfare of our citizens. Like generals who blindly prepare for the last war, our economic policy-makers spend too much of their time thinking about the last economy.” House of Representatives, Committee on Banking, Finance and Urban Affairs, Subcommittee on Economic Stabilization, *Service Industries: The Changing Shape of the American Economy* (Govt Printing Office, 1984), quoted in Karl P. Sauvart, *International Transactions in Services: The Politics of Transborder Data Flows* 2 (Westview Press, 1986).

3. See generally John B. Shoven, *Intellectual Property Rights and Economic Growth*, in Charles E. Walker & Mark A. Bloomfield, eds, *Intellectual Property Rights and Capital Formation in the Next Decade* 46 (U Press of America, 1988); Frank H. Easterbrook, *Intellectual Property is Still Property*, 13 Harv J L & Pub Pol 108 (1990).

Information is intangible. Although it may be recorded in an object or on paper, the tangible embodiment is not the information itself, nor does it determine who knows or can use it. Thus, thousands of people can “possess” one piece of information at the same time; possession, if one uses the term regarding information as a product, merely implies that a person knows of and understands the data. For goods, by way of contrast, the idea of possession refers to *physical* possession and has various practical and legal connotations with respect to controlling, protecting, and transferring the item.

Unlike goods, information can be used without being used up and can be sold without being given up. One can sell and “deliver” information to another but still retain the information in his possession and for his own personal use. This is not, of course, the case in the sale of a tangible product. If one sells and delivers a television set to another, though he can purchase a replacement, he no longer possesses nor can he use the set that he sold.

The distinctive nature of property rights in information shapes the contract terms that are critical to commercializing an information product. To approximate the characteristics of the sale of a tangible item, a transfer of information must entail restraints on the seller that are created by law or by some form of an agreement. If one wishes to buy information that one alone will own and control, one must exact from the seller an undertaking neither to use the information nor to convey it to another person. Even if one receives this assurance, not only may others obtain the same information from other sources, but there is a continuing risk that the seller will breach its agreement, leaving one only with a right to enforce one’s property right of exclusivity.

Accordingly, it is clear that commercial law concepts of sale or lease of goods cannot be applied directly to transactions in information. The ideas of sale or lease of goods presuppose tangible items inherently distinguishable from others of similar type. Even though millions of red Toyotas exist, the particular Toyota one may purchase is unique—one owns it. This cannot necessarily be said of information that one may buy. Hence, conventional ideas about transfer—giving to another and relinquishing control—need to be modified when one is dealing with information. In the context of information, one can discuss exclusivity or a right to continued use. In contracts that define the “sale” of information, these terms define the property transferred. The “purchaser” must determine whether she bought exclusive use or mere knowledge and a right to use coequal with that retained by the seller.<sup>4</sup>

---

4. In many developed countries, trade in information exceeds in importance trade in goods. Information products and providers include:

periodical publishers	newsletters
book publishers	securities analysts
database providers	newspapers
magazines	computer networks
encyclopedias	literature searches
title insurance	service directories
telephone directories	professional listings
white pages	labor listings

Understanding the most fundamental similarity among these various products requires an appreciation of the distinction between data and information. Data are signals, symbols, or at most discrete facts. Data become information only when an individual, a group, or tradition attributes a meaning to them. The letters "LEXIS" are data. They comprise information only if we accept or are made aware that they signify a law-related database. Knowledge comes from the use of data and their association into patterns incorporating judgments and interpretations.<sup>5</sup>

All information products communicate data, but their value lies in that they do so with an eye toward the audience to which they are directed. The products convert data into information or into a form from which the end user can glean information. The author of an article interpretatively transforms raw data into a story. An editor selects the data that are communicated to readers of a newspaper and the form in which they appear. An economist produces an evaluative report based on data and on an understanding of theory, politics, and trends relevant to a particular audience. An accountant sorts financial data into categories determined by accounting standards. An opinion survey designs questions, collects data, and tabulates results to determine the buying or voting public's attitudes. Finally, a bookmaker tabulates, gives information, and collects money.

Information products primarily convert data into information. This requires creative skill or effort from the information supplier or the data recipient. An information supplier's goal is to fit data into the users' frame of reference. Unless data make sense to the end user, they inform no one of

---

yellow pages  
abstracting services  
economic consultants  
indexing services  
forecasting services  
current awareness services  
clearinghouses  
medical treatment information  
census  
parts catalogues  
real estate multi-lists  
clerical functions  
bookmaking services  
land surveys

sports statistics  
document acquisitions  
environmental consultants  
mailing lists  
records management  
management consulting  
financial market data  
opinion surveys  
market analyses  
engineering information  
horoscopes  
accounting services  
television news  
astronomical charts

Adapted from Carlos A. Cuadra, *The Role of the Private Sector in the Development and Improvement of Library and Information Services*, 50 Library Q 98 (Jan 1980). While these products range across most aspects of modern life, they share a quality of communicating selected or comprehensive information to subscribers or buyers. They exhibit sharp differences as well as striking similarities in format, however.

5. Wurman described the need to organize data to fit the reader's perspective as a necessary means to alleviate information anxiety and as an inherent element of converting data to information:

Raw data can be, but isn't necessarily, information, and, unless it can be made to inform, it has no inherent value. It must be imbued with form and applied to become meaningful information. Yet, in our information-hungry era, it is often allowed to masquerade as information . . . . Information must be that which leads to understanding. Everyone needs a personal measure against which to define the word. What constitutes information to one person may be data to another.

Richard Saul Wurman, *Information Anxiety* 38-39 (Doubleday, 1989).

anything.<sup>6</sup> Information products thus involve data compilation, judgment, and structure—essentially, they incorporate a services component. One might construe this as value-added activity, but more correctly, it constitutes an inherent feature of information as a product. An information product inseparably involves both an object—intangible though it may be—and an interpretation—accurate or inaccurate as it may be.<sup>7</sup> In intellectual property law, the relationship between information and creative services provides a fulcrum on which law balances proprietary rights and public use. Proprietary rights are attributed to the judgment or structure, but not to data that are publicly disseminated.<sup>8</sup> For commercial law, this distinction defines which products the parties can buy, sell, or license, and how this can be done.

Technology plays a role in defining modern information products, but that role differs among different products. In many cases, the information product existed before computers came on the scene, and the technology merely makes creation or dissemination of the product less cumbersome—such as in the case of a national newspaper. In other cases, however, the electronic systems enhance the product, making it more flexible and responsive to the needs of particular users. A product consumer can more readily reorganize, modify, and manipulate electronic products, such as an electronic database, than tangible products or even information products sold in tangible media, such as an encyclopedia. At some point, this greater flexibility may create an entirely different commercial product. The product then exists *because* the electronic systems make it possible.

Digital data-storage technologies change the number of ways in which data can be altered, examined, summarized, and restructured to produce new or newly tailored information.<sup>9</sup> If one, for example, receives a casebook in electronic form, one can rearrange chapters, add cases, and make other

---

6. *Id.* at 39.

7. Edmund Kitch was one of the first to recognize this aspect of information products and to connect the services (or personality) aspect of valuable information with the ease or difficulty by which one can take the information. He argued, among other things, that information is self-protecting and difficult to steal because information within a company (largely trade secrets) is “embedded in a context that contains a great deal of extraneous information.” Edmund W. Kitch, *The Law and Economics of Rights in Valuable Information*, 9 J Legal Studies 683, 712 (1980).

8. As information becomes increasingly valuable, we witness a sharp increase of litigation testing the boundaries of this distinction. See, for example, *Feist Publications, Inc. v Rural Telephone Service Co.*, 111 S Ct 1282, 1296-97 (1991) (names, towns, and telephone numbers in white pages are not copyrightable); *Victor Lalli Enterprises, Inc. v Big Red Apple, Inc.*, 936 F2d 671, 673 (2d Cir 1991) (charts summarizing winning numbers in New York’s gambling operations according to functional grids are compilations of preexisting facts and therefore not copyrightable); *BellSouth Advertising & Publishing Corp. v Donnelly Information Publishing, Inc.*, 933 F2d 952, 958 (11th Cir 1991) (holding the format of BAPCO yellow pages, which uniquely compiled businesses into numerous business selections, was protected under the copyright laws); *Kregos v Associated Press*, 937 F2d 700, 709 (2d Cir 1991) (copyright can protect only selection of statistics for baseball pitcher statistical compilation, not garden variety arrangement of statistics); *Kern River Gas Transmission Co. v The Coastal Corp.*, 899 F2d 1458, 1463-64 (5th Cir 1990) (since the idea of building a pipeline is not copyrightable, the expression of the idea via maps, inseparable from the idea itself, is also not copyrightable under the merger doctrine).

9. See generally Office of Technology Assessment, *Intellectual Property Rights in an Age of Electronics and Information* (Govt Printing Office, 1986) (“OTA, *Intellectual Property Rights*”).

changes before using it. Whether one has the *right* to do so is a question of law and legal policy, but the medium supplies the capability. Similarly, for a credit card company that maintains a database of customer transactions that enables it to bill and collect charges, the fact that the company can re-examine the data in a computer rather than in file folders means that the company can re-examine the database and sell the information derived concerning buying habits and trends to vendors of other goods and services. Whether the credit card company can do this legally or contractually is a question of evolving modern concepts of electronic property rights.

Many would argue that electronic data systems make information more accessible to end users. But this may be too facile a conclusion. Electronic databases create greater availability than do their published counterparts in some ways, but they are less accessible in others. Clearly, one's ability to dial Prodigy from home gives greater access to the contents of that database than one has to the volumes in a library miles away.<sup>10</sup> On the other hand, any law firm that subscribes to WestLaw is aware that the hourly use charges create a different cost basis and accessibility than the cost of a set of books. Once a buyer purchases an encyclopedia, the buyer owns that copy and has free and unlimited access to all the information it contains. However, the buyer cannot ordinarily purchase information in an electronic database in this same sense. The subscriber purchases only a right to access and endures a further charge each time that right is exercised. The database contract transfers a right of access to information; the encyclopedia sale transfers information ownership identical to the ownership rights enjoyed by all other purchasers of the same book. This difference in rights transferred affects the intellectual property law balance between encouraging public disclosure and dissemination on the one hand and a system of property rights and incentives on the other; the balance point changes from a right to make and sell copies to a right to control access.<sup>11</sup> In essence, the predominant property right sought by the vendor of an electronic database system relates to the power to allow or deny others access to that database, while the property right of greatest importance to the book publisher relates to the power to prevent others from copying and selling copies of the book.

All commercial exchanges involve legal assumptions about the seller's right to make a transfer and to convey the value exchanged. The importance of these assumptions is especially great in transfers of information because the practical advantages of physical possession cannot be substituted for legal control where more than one party handles the information. The legal assumptions that must be true in order to traffic commercially in information differ depending on the type of product, but some common features exist.

---

10. See generally John F. Wasik, *The Electronic Business Information Sourcebook* (Wiley & Sons, 1987) (listing numerous database systems available at that time and describing these as "the best workshop of research tools the world has ever known").

11. OTA, *Intellectual Property Rights* (cited in note 9).

These can be understood by considering two facets of information products: the method of distribution and the subject matter.

#### A. Method of Distribution

Information products are offered to the general public for commercial use in various ways along a continuum of increasing availability. At one end is the closely restricted or secret information held within a company and kept from others by security restrictions and contract restraints.<sup>12</sup> Some of this information may be transferred to persons outside of a company, but often the terms of the transaction restrict further disclosure or use of the information in order to retain the value achieved through secrecy. At the other end are general distribution products that are disseminated broadly and without substantial restriction on an open market. Among these are newspapers, books, and broadcast television or radio. Between these extremes are numerous degrees of limited distribution products on which the vendor's economic return comes from charging for intermittent or limited access—such as a private marketing survey.

Each type of product works in the marketplace for different reasons. Obviously, the success of a product depends in part on its ability to provide desired information in a useful form for a sufficient paying audience. The nature of the public and the return on investment sought, however, vary widely, and these variations affect the legal rights that are important to the commercialization of the information product. A newspaper publisher sells many copies at a low price over a short time, supplementing his profit by selling advertising space in each publication. By way of contrast, a book publisher or author depends for profit on his ability to sell fewer copies at relatively higher prices over a longer period of time and, in many cases, to sell as well different rights to reproduce the book in paperback, in a foreign language, or as a motion picture. These products rely for profitability on different shelf-life expectations and on control of different aspects of the right to use or reproduce the information contained in the products. The different shelf-life expectations of the two product types affect the relative importance attached by the information vendor to legal protection against copying

---

12. Trade secrets form the core of one of the major fields of intellectual property law. See Roger Milgrim, 12 *Business Organizations: Milgrim on Trade Secrets* (Matthew Bender, 1986); *Ruckelshaus v Monsanto Co.*, 467 US 986 (1984) (addressing whether EPA's disclosure of trade secrets, submitted by Monsanto pursuant to the federal Insecticide, Fungicide & Rodenticide Act, were takings without compensation); *Rockwell Graphic Systems, Inc. v DEV Industries, Inc.*, 925 F2d 174, 180 (7th Cir 1991) (it is an issue of fact whether manufacturer of printing press part design took reasonable steps to protect its trade secrets, thus precluding summary judgment); *Eden Hannon & Co. v Sumitomo Trust & Banking Co.*, 914 F2d 556, 560 (4th Cir 1990) (investor breached nondisclosure agreement with analyst by bidding on target project), reh'g denied, reh'g en banc denied. When held by an individual about that individual, courts will more often treat the information as entailing an issue of privacy law, defined here as the question of to what extent an individual owns attributes of control in information about her own personal life. See discussion in *Finger v Omni Publications Intl, Ltd.*, 566 NE2d 141, 144 (NY 1990) (publication of photograph of family with six children, without their consent, did not violate their privacy rights because the photograph related to the newsworthy theme of the article that caffeine can increase a man's fertility).

published material, legal protection against premature disclosure, and legal protection of access to the information contained in the work.<sup>13</sup> The vendor of the shorter shelf-life and lower cost-per-unit product is commonly less concerned with copying since, owing to the economics and timing of the matter, the copying competitor poses only a slight threat to the product's commercial success. This vendor will often be much more concerned, however, about the right to control first publication of particular information. The vendor of the longer shelf-life product, on the other hand, stands to suffer much more commercial injury if some competitor copies the product's content and takes a market position without needing to incur the initial research, writing, or other costs required to produce the information product. What these vendors sell—and the property rights on which they rely—differ, even though both deal with information products.

A company holding secret information may profit from that information by keeping it entirely within the firm or by transferring some rights in the information to third parties. The third parties may provide services for the information owner or may themselves use the information for their own purposes. In any case, the economics of secret information depend on the ability to make restricted disclosures. This, in turn, hinges not only on security systems, but more importantly on laws that permit or prohibit restrictions. Thus, a company that investigates oil reserve structures in the North Atlantic may profit by selling information to Shell and perhaps Exxon. Both the initial and the continuing value of the information to the company and to the selected buyers will depend on the ability of each party to restrict access to the information and, once disclosed, to restrict use and further disclosure.<sup>14</sup>

Electronic information products fall at various points along this continuum, reflecting the diversity of the technology. Many book publishers use electronic formats—that is, diskettes—to distribute reference books. Except for the fact that to “read” these diskettes requires special equipment, the product is like a traditional book in terms of the legal conditions that make distribution potentially viable as an economic matter. These presumed conditions are that either law or contract prevents the buyer from making multiple copies of the disk. The technology here changes or eliminates practical obstacles to copying, but it does not change the legal framework. Similarly, electronic systems may also be used to store and control access to secret information.

---

13. On the issue of the cost of premature disclosure of a book publication, see *Harper & Row, Publishers v Nation Enterprises*, 471 US 539 (1985) (holding that it was not a fair use to copy excerpts of an unpublished manuscript for commercial gain).

14. See, for example, *Sunds Defibrator AB v Beloit Corp.*, 930 F2d 564, 566 (7th Cir 1991) (distinguishing between use and disclosure as elements of control dealt with under a disclosure agreement); *Rockwell Graphic Systems*, 925 F2d at 177 (ability to transfer to third-party support companies and yet retain control is critical factor in using secrets); *Eden Hannon*, 914 F2d at 558 (value of firm depends on its information).

Electronic technology is also at the center of cable and other mass television systems. The technology here services either a broadcast format with no restrictions on receipt of the information signal or one with a signal requiring special receiving equipment. The latter format allows creation of a widely distributed but limited access product that, as a viable product framework, depends not only on the technology, but also on the assumption that underlying law allows the use of the encrypted signals that typify this technology and bars unauthorized access to the signal by third parties.<sup>15</sup> A legal right to prevent copying such products also has value in that copying this type of information under copyright and communications law equates with the act of receiving and recording the received signal.

The cable illustration suggests that one aspect of new technology products creates a potential for broad but still restricted dissemination. This potential is seen also in electronic database systems that provide data collections that are continually updated and refined. These systems regulate access and charge for both the right to access and the duration of any particular access to the system. The profitability of this type of product obviously depends on the enforceability and legality of access restrictions through technology.<sup>16</sup>

## B. Subject Matter

Information products also differ in their subject matter. The following four variables capture most of the variety:

- (1) *How the data are collected:*
  - as a by-product of another activity
  - as a goal of data collection
- (2) *The subject of the information:*
  - individuals
  - businesses
  - techniques/technologies
  - governments
  - society patterns
- (3) *The circulation of the constituent facts:*
  - private facts (very limited circulation)
  - public facts (very wide, prior circulation)
- (4) *The form of the information:*
  - summarized (group) data (e.g., statistics)
  - analyzed by provider (e.g., report)
  - raw data organized by specific traits (e.g., name)
  - raw data unorganized

---

15. Both circumstances have evolved in our law. See, for example, *Home Box Office, Inc. v Corinth Motel, Inc.*, 647 F Supp 1186, 1190 (ND Miss 1986) (unauthorized reception of cable transmission and subsequent provision to hotel guests violates copyright and communications act). Compare *National Football League v McBee's & Bruno's, Inc.*, 792 F2d 726 (8th Cir 1986).

16. See, for example, *United States v Morris*, 928 F2d 504 (2d Cir 1991) (criminal prosecution for unauthorized access to computer network); *Telerate Systems, Inc. v Caro*, 689 F Supp 221, 226-31 (SD NY 1988) (copyright violation for accessing and copying parts of the database).

The blending of these four variables in different ways can produce vastly different subject matter products. These differences can also raise entirely different policy issues regarding ownership rights and quality assurances. For example, credit card data collected as a by-product of individuals' card use represents a marketing resource of private facts that are not widely known. If distributed in a form that compiles the data by consumer name, the product supplies information about the individual and raises privacy law concerns. Privacy deals with information ownership. Who has the right to distribute products that reveal private information about individuals? Alternatively, distribution in a form that compiles the data by the name of those businesses at which items are purchased conveys information about sales and customer lists of those businesses, which many retail companies treat as trade secrets. Who has the right to such information when it is held in the credit card system? As a third possibility, the information may be distributed as a general summary of market areas. Here, the absence of individualized attribution of the data makes it easier to conclude that the information is owned by the credit card company, which gives that company a highly valuable asset from which it can produce numerous sellable market study reports.

For each of these variations, there are not only questions about ownership of the information distributed, but also questions about who bears the risk of its inaccuracy. If the credit card company sells miscalculated market data to Macy's, which opens a new store in reliance on the data, is the company liable? If so, for breach of what standard of care or quality? Or if the data describing individual companies are published in a book on local retailing patterns, can Bloomingdale's recover for an error that underestimates its profitability by seventy-five percent? The manner of distribution affects the liability standard, with broadly published information less likely giving rise to liability for inaccuracy than the selectively distributed product.

Consider another group of information products: an opinion survey among attorneys about the political attitudes and professional abilities of criminal court judges in a county. This information, which was collected with the goal of obtaining information about government, constitutes otherwise private facts that can be distributed in summary form. The survey company assumes that it has the legal right to retain possession of the facts collected and further assumes—and may have so assured attorney respondents—that the company can conceal the individual responses about individual judges. If the company cannot enforce these rights, it may not be feasible to create the summary product, since the attorney respondents may refuse to respond to the survey. The right to control disclosure of the survey answers involves assertion of a right of ownership. Indeed, the survey company would face the same property rights issue if it decided to publish the results not by the judges' names, but alphabetically by the attorneys' names. The issue there would be whether the attorneys could prevent publication—that is, disclosure. On the other hand, if the survey results—either the summary or the individual listings—contain inadvertent errors, this raises an issue of product quality

assurance. What are the rights of the party who purchased the survey, the judge whose skill is misrepresented, or the attorney whose opinion is not accurately described?

Consider now a company that conducts research on the profitability, client base, and performance record of law firms. It examines public records, including court files, and in cases where the information is available (for example, bankruptcy court records), the company records. It publishes in book form the fees awarded by the court, the win-loss record, client names, and other data arranged by attorney and by law firm. The attorneys and their law firms do not, one expects, own the information contained in public records in the sense that they can prevent the company from locating and publishing these data,<sup>17</sup> for they are in the "public domain." Do the attorneys and their law firms then have a right to recover for misstated facts that damage their ability to obtain or retain clients? What property rights and protections against liability are necessary or desirable to shield the company that produces this general distribution product?

Possible combinations of variables drawn from information products already in commercial operation are endless, but the foregoing illustrations adequately make three fundamental points. First, just as the content of a product affects legal policy issues, so does the chosen method of its distribution. Second, the same data, especially in electronic form, can be molded into numerous different products, each of which raises different ownership and quality concerns. And finally, these illustrations show quite clearly that knowledge of information does not imply ownership, at least insofar as ownership entails an unfettered right to use information. Ownership of some attributes of information can vest simultaneously in the person who knows the information, the person to whom the information pertains, and the person who "sold" the information.

## II

### INFORMATION AS PROPERTY

Treating information as commercial property that can be sold, exchanged, or transferred conditionally requires a definition of the concept of "property" in this context and the limits or conditions that the law places on that concept. In its broadest connotation, the idea of information as property refers to the bundle of rights that can include the control of copying, access, modification, use, and disclosure of data and information. These property rights do not exist in all cases, however, and in any event, they exist in varying degrees, depending on the nature of the information, its location, and its contemplated

---

17. A different circumstance may exist in cases where the company seeks to obtain such information from a governmental record which, in itself, summarizes in computer form the disparate items of "public information." See *United States Department of Justice v. Reporters Committee for Freedom of the Press*, 489 US 749 (1988) (holding that a third party could not obtain FBI rap sheets on named individual under the freedom of information law because of the privacy exemption, even though the individual records were public).

or previous use. Indeed, the existence of these rights derives from several different bodies of law, the interrelationship among which is often not clearly perceived.

Independent of the content or location of information, the definition of a property right therein determines what one party may trade or sell to another. In essence, the property right defines the character and content of the commercial transaction. Additionally, as mentioned earlier,<sup>18</sup> information products may entail elements of contracting for services; thus, even absent any property right in the information itself, this service component may constitute a potentially tradable right in a commercial relationship. In part, at least, the law of information property rights and information as a focus of a commercial transaction incorporates the law of contracts for services.

#### A. Copyright and the Public Domain

The law favors the release of factual information into the public domain along with free access to and use of the information thus disclosed. On the other hand, there is an increasingly strong tendency in law to protect secrecy and confidential relationships. These competing principles affect the development of property rights in information products.

Unless a piece of generally disseminated information qualifies for patent law protection for the technology it describes, our law narrows both property rights and liability risk in the public domain. This enables readier access and broader use. But however narrowly drawn, property rights in public domain information are recognized in our law. The absence of all property right protection in a general distribution product would yield underproduction of important information products, since the producer would have inadequate economic incentives to invest in new information products.<sup>19</sup> Thus, granting at least some property right to the producer of information is seen as consistent with the goal of promoting the development of a public domain information base.<sup>20</sup>

---

18. See discussion generally at notes 6-8 and accompanying text.

19. Wiley describes this as the consumer approach to justifying intellectual property law and contrasts it to what he describes as a producer-oriented approach, which justifies such protection based primarily on fairness to the producer of information. John Shepard Wiley, Jr., *Copyright at the School of Patent*, 58 U Chi L Rev 119, 138 (1991). Compare discussion in Wendy J. Gordon, *An Inquiry into the Merits of Copyright: The Challenges of Consistency, Consent, and Encouragement Theory*, 41 Stan L Rev 1343 (1989).

20. This goal is also visible in the evolution of patent law, a traditional element of which has been described in terms of inducing an inventor publicly to disclose her invention in patent files in return for very robust property rights to control applications and use of that invention other than for further research. See Rebecca S. Eisenberg, *Patents and the Progress of Science: Exclusive Rights and Experimental Use*, 56 U Chi L Rev 1017 (1989) (comparison of the competing rationales behind exclusive patent rights and broad access to scientific discoveries in analyzing the experimental use exemption to patent infringement). See generally Kitch, 9 J Legal Studies at 683 (cited in note 7). As is true in many aspects of intellectual property law theory, there is no clear proof that the scientific community actually benefits from disclosure, or that those benefits actually attained are commensurate with the high cost of the patent system. See Robert P. Merges & Richard R. Nelson, *On the Complex Economics of Patent Scope*, 90 Colum L Rev 839, 871-78 (1990).

Copyright law dominates the law of property for generally disseminated information. Although it withholds any property right in facts and data, copyright law does grant the information producer a limited property right in one aspect of the services feature of the product—namely, the form in which the data are compiled, arranged, or otherwise “expressed,” if that expression is “original” to the particular author. This property right is largely concentrated in the right to control copying of the work and does not necessarily provide protection of a right to control access, disclosure, or use.

In 1991, the Supreme Court in *Feist Publications, Inc. v. Rural Telephone Service Co.*<sup>21</sup> denied copyright protection to either the data or the arrangement of the data in a white pages telephone directory. A telephone directory, of course, is a fact-intense, widely distributed product whose value derives from its accessibility over an extended period. In leaving this product unprotected against copying, the Court emphasized and restated a traditional limit of law: copyright cannot create proprietary control in factual data, but only in how facts are expressed.<sup>22</sup> In essence, regardless of how difficult or costly the collection and assembly of factual material has been or how elegant the expression of this material may be, copyright protection does not enable the author to prevent others from copying those facts. It is also true that copyright does not generally create any right to prevent others from using or disclosing the facts or expression to others if this occurs without copying the expression.<sup>23</sup>

Although it is possible to use copyright law to prevent another from copying how one organizes and expresses facts—that is, how they are converted into information—*Feist* further held that the alphabetical arrangement of names in a white pages directory was too obvious and commonplace to constitute the original expression required by the statute.<sup>24</sup> The flaw in the *Feist* product from a copyright perspective was that the data were comprehensive, indicating no creative selection for inclusion, and their (alphabetical) arrangement was common. This combination of product definition choices was fatal to the claim of a copyright property interest in the commercial product.

---

21. 111 S Ct 1282 (1991).

22. *Id* at 1289.

23. This principle flows from the basic nature of copyright law, but has potentially significant limits under current copyright doctrine. For example, several courts have held that the copyright grant to an author of the exclusive right to make a derivative work from her original includes use of the original in modified form, even though that use does not entail making an additional copy of the work. See *Mirage Editions, Inc. v Albuquerque A.R.T. Co.*, 856 F2d 1341, 1343 (9th Cir 1988) (holding that individual who mounted copyrighted artworks on tiles and sold them to the public prepared derivative works, which infringed those copyrights); *Midway Mfg. Co. v Arctic Intl, Inc.*, 704 F2d 1009, 1014 (7th Cir 1983) (holding that defendant who sold circuit boards that accelerated plaintiff's copyrighted video games supplied a derivative work, which infringed the copyright). Similarly, in the field of computer software, the distinction between use and copying has been perhaps irreversibly blurred by the fact that loading a program into a computer for use constitutes making a new copy of it. See Raymond T. Nimmer, *The Law of Computer Technology* ch 1 (Warren, Gorham & Lamont, 2d ed 1992).

24. *Feist*, 111 S Ct at 1296.

Rural simply takes the data provided by its subscribers and lists it alphabetically by surname. The end product is a garden variety white pages directory, devoid of even the slightest trace of creativity. Rural's selection of listing could not be more obvious . . . . Rural expended sufficient effort to make the white pages directory useful, but insufficient creativity to make it original.<sup>25</sup>

Copyright protects only original expression. Factual data, however discovered and however difficult to find, are not original to the author.

*Feist* preserves a public domain of freely available information and favors protection of that domain over the protection of a publisher who may have expended substantial resources creating an information product. One can argue that on *Feist's* particular facts, there was no reason to allow copyright protection as an incentive to create a directory. For telephone companies, the white pages consist of data obtained as a by-product of business; indeed, the company must produce the data in some form to enable its business to continue. The Court did note this point, but the scope of its ruling is far broader and not confined to this narrow factual context.

In *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*,<sup>26</sup> the Supreme Court also emphasized that a public domain of unprotected factual information exists. There the Court indicated that legally guaranteed free access to and use of generally distributed data that are not protected by patent or copyright law constitutes part of the "intellectual property bargain," which grants exclusive property rights to certain information in order to create incentives for its general disclosure. This bargain, however, "depend[s] almost entirely on a backdrop of free competition in the exploitation of unpatented designs and innovations."<sup>27</sup> The Court went on to invalidate a state law that attempted to alter this bargain by granting the designer of a boat the right to prevent others from copying the hull design through a process of direct molding, on grounds that the state law created exclusive rights in information in cases where federal law denied them.<sup>28</sup>

*Feist* generated an immediate string of decisions dealing with the conditions under which courts will extend or deny copyright protection to

---

25. See generally Jane C. Ginsburg, *Creation and Commercial Value: Copyright Protection of Works of Information*, 90 Colum L Rev 1865, 1924-36 (1990) (arguing that authors whose compilations of data are held unoriginal should nonetheless be protected by a compulsory license, which gives competitors access to the information after they first pay a fee to the original compiler); L. Ray Patterson & Craig Joyce, *Monopolizing the Law: The Scope of Copyright Protection for Law Reports and Statutory Compilations*, 36 UCLA L Rev 719 (1989) (disagreeing with the *West Publishing* court's decision to grant West a monopoly over star-pagination). Compare Robert C. Denicola, *Copyright in Collections of Facts: A Theory for the Protection of Nonfiction Literary Works*, 81 Colum L Rev 516, 530 (1981).

26. 489 US 141 (1989).

27. *Id.* at 151.

28. *Id.* at 159-60. This holding did not invalidate rules that allow contracts or special relationships to impose restrictions on particular parties, nor did it invalidate the idea that the mere possibility of acquiring a secret from a distributed product allows the purchaser to breach its covenant of confidentiality. See, for example, *Boeing Co. v. Sierracin Corp.*, 738 P2d 665, 674-75 (Wash 1987) (en banc) (aircraft window supplier misappropriated designer's secrets despite conflicting evidence that windows could have been reverse engineered); *Data General Corp. v. Digital Computer Controls, Inc.*, 357 A2d 105, 113 (1975) (taking information from confidential documents actionable even though one could have discovered secret from machine that was purchased).

products whose function is to report factual data in understandable form. In *Victor Lalli Enterprises, Inc. v. Big Red Apple, Inc.*,<sup>29</sup> for example, the Second Circuit denied copyright protection to a published chart of horse-racing figures covering a thirteen-month period. These data were unprotected facts, and how the publisher organized or expressed these data in the chart was dictated by long-standing convention. Merely arranging factual information into “purely functional grids that offer no opportunity for variation” cannot achieve copyright protection.<sup>30</sup> By way of contrast, however, in *Kregos v. Associated Press*,<sup>31</sup> the same court granted copyright protection to a reporting format that combined into one cluster a set of nine statistics on baseball pitchers, where the grouping of the statistics was different from that included in other reporting systems.

Copyright law allocates only a limited property right for information products—generally the right to make copies of the work. *Feist* denies that property right to some information products, particularly those that report relatively pure factual data. The telephone directory, the horse-racing data, and the baseball statistics all have value, but all of these products report purely factual data whose value stems from their collection in one place and their resulting availability to an end user. Although collecting information can be both costly and time-consuming, such industry alone does not qualify the product for the protections created by copyright law.

*Feist* defines the nature of information products by disallowing copyright protection for the effort expended in collecting and for “obvious” organizations employed in conveying information. Since the right to control copying is denied, what remains available for commercial sale must come from other sources of value in the product. The collection of facts in a directory, for example, retains value because of its convenient arrangement of useful information. The person who has collected and published the information has rendered a service in developing the product. Although a valuable product remains, its property attributes are different from those that would have been conferred by copyright; denial of copyright changes what the information provider sells and how the provider commercializes the product. The information provider can still sell the service of collecting and reporting data and delivering the product of that service in a particular form, but it cannot prevent others from copying the product. The value of the service without the right to prevent copying determines the commercial value of the product.

*Feist* and *Bonito Boats* deal with products placed on the open market and with the right to copy aspects of such products. For other information products, however, the *right to copy* is less singularly important. Other property rights dominate, such as the rights to restrict access, to control modification, and to control disclosure or use. These rights are not available

---

29. 936 F2d 671 (2d Cir 1991).

30. *Id.* at 673.

31. 937 F2d 700, 704-05 (2d Cir 1991).

for published and widely disseminated products either as a matter of fact or as a matter of law, but they are often the most important property rights in limited distribution products, including electronic databases.

The right to control another's access to information can implicate several distinct bodies of law, including the law of trade secrets, criminal law, communications law, and various laws relating to privacy interests. Considering all of these factors together, the access control right depends on the presence of one or both of two factors: (1) holding the records of the information in a place defined by law as secure or protected; and (2) disclosing that information in a relationship defined in law and in practice as confidential in character.

## B. Access and the Computer

During the last decade, various criminal and communications law reforms have established that a computer environment constitutes a protected zone, unauthorized access to which constitutes a crime in the nature of trespass. During the 1980s, forty-eight states and the federal government enacted computer crime legislation.<sup>32</sup> Illustrative is the Illinois statute:

It is the intent of the Legislature . . . to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems.<sup>33</sup>

Most of these statutes treat unauthorized access as the primary criminal act, but they condition sanctions on what occurs after the access is achieved.<sup>34</sup> The statutes typically define access in general terms, such as "to instruct, communicate with, store data in, or retrieve data from, a computer, computer system or computer network."<sup>35</sup> Federal computer law parallels this approach, treating access as a primary right in the Computer Fraud and Abuse Act.<sup>36</sup>

---

32. See Eli Lederman, *Criminal Liability for Breach of Confidential Commercial Information*, 38 Emory L J 921 (1989) (extensive discussion of computer crime and criminal trade secret statutes that tracks the extent to which legislatures and courts have shifted their focus toward protecting information as an intangible regardless of the tangible manifestation of that information).

33. Cal Penal Code § 502(a) (West, 1992).

34. Thirty-eight states have criminalized unauthorized access to a computer or the data contained therein, at least in some forms, most often as part of a general list of computer crimes. See 5A Ariz Rev Stat Ann § 13-2316 (West, 1989); Del Code Ann Tit 11 § 935 (1987); Ga Code Ann § 16-9-93 (Michie, 1991); Mich Comp Laws § 752.795 (1991); NM Stat Ann § 30-45 (1989); NC Gen Stat § 14-454 (1986); ND Cent Code § 12.1-06.1-08 (Supp 1991); RI Gen Laws § 11-52-2 (Supp 1991); Tenn Code Ann § 39-14-602 (1991); Utah Code Ann § 76-6-703 (1990).

35. 11 Del Code Ann § 931(1) (1987). Even the most common definitions are non-uniform, however. For instance, unauthorized access under the Maryland Code, Md Code Ann art 27 § 146(c) (1992), is equivalent to computer trespass under the Washington statute. Wash Rev Code § 9A.52.110 (1988). In some states the terms "access" and "use" are interrelated. Hawaii defines "access" as the "use of any resources of a computer, computer system, or computer network," Hawaii Rev Stat § 708-890 (1988), while Mississippi defines "access" as "to program, to execute programs on, to communicate with, store data in, retrieve data from, or otherwise make use of any resources . . . ." Miss Code § 97-45-1[a] (1990).

36. 18 USC § 1030 (1988). The Act establishes criminal penalties for stealing national security related data, for trespassing onto government computers, and for stealing computerized information

Unauthorized access is analogous to trespass. The owner of property has an inherent right to exclude other persons. Clearly, however, physical trespass is not identical to unauthorized access. "[Trespass] statutes criminalize the entering and remaining upon premises [while] computer trespass . . . criminalizes the entry into the computer base . . . ." <sup>37</sup> Trespass entails physical entry, but electronic access does not. <sup>38</sup> Access crimes, therefore, constitute an expansion of traditional property concepts into an electronic milieu. <sup>39</sup> More importantly, they provide a foundation for the legal protection of new commercial products and systems.

In *United States v. Morris*, <sup>40</sup> the Second Circuit affirmed a conviction under the Computer Fraud and Abuse Act <sup>41</sup> for the crime of unauthorized access to a federal interest computer causing damage, alteration, or destruction of information in that computer system or preventing authorized use of that information. Morris had paralyzed a computer network by inserting a "virus" into the network, which for a time effectively disabled the operation of the system. The Court rejected Morris's argument that the criminal offense required an intent to cause harm, noting that the only intent required was merely the intent to access the system without authority. <sup>42</sup>

---

on individual credit histories. Id § 1030(a)(1-3). The act also covers three offenses associated with unauthorized access to federal interest computers at least where that access has the intent or necessary result of causing damage or yielding a theft of property. These are: (1) access with the intent to defraud resulting in the taking of value; (2) intentional access that alters, damages, or destroys information; and (3) trafficking in access passwords. Id § 1030(a)(4-6). "Federal interest" computer is defined as a computer that is (1) exclusively for the use of a financial institution or the U.S. Government or, if not exclusively so used, the offense affects the portion of the system so used, or (2) one of two or more computers used in the offense, not all of which are located in the same state. Id § 1030(e)(2).

37. *State v. Olson*, 47 Wash App 514, 735 P2d 1362, 1364 (1987).

38. See *American Computer Trust Leasing v Jack Farrell Implement Co.*, 763 F Supp 1473, 1493-94 (D Minn 1991) (remote deactivation of licensed software was not actionable).

39. A debate about a similar expansion exists in reference to theft law. In *United States v Riggs*, 739 F Supp 414 (ND Ill 1990), a scheme to obtain electronically the computer text file for "911" numbers, transmit it across state lines by computer network, and publish it in a newsletter resulted in charges under the federal Stolen Property Act, 18 USC § 2314 (1988). The Supreme Court had held in *Dowling v United States*, 473 US 207 (1985), that the act did not apply to actions of mere copyright infringement, but that cases under this Act must involve "physical goods." *Riggs* formulated an electronic definition of property covered by the act:

[The] computer-stored business information in this case satisfies [any] requirement [of tangibility]. Although not printed out on paper, a more conventional form of tangibility, the information [was] stored on computer. Thus, by simply pressing a few buttons, [defendant] could recall that information from computer storage and view it on his computer terminal. The information was also accessible to others in the same fashion . . . . This ability to access the information in viewable form from a reliable storage place differentiates this case from the mere memorization of a formula and makes this case more similar to cases . . . where proprietary information was also stored, but in a more traditional manner—on paper. The accessibility of the information in readable form from a particular storage place also makes the information tangible . . . .

*Riggs*, 739 F Supp at 422. *Riggs* was rejected by the court in *United States v Brown*, 925 F2d 1301, 1308-09 (10th Cir 1991) (Act does not apply to the theft of a computer program in source code form).

40. 928 F2d 504 (2d Cir 1991). See also *Burleson v State*, 802 SW2d 429 (Tex App 1991) (conviction for harmful access to computer under state law).

41. 18 USC § 1030(a)(5)(A).

42. *Morris*, 928 F2d at 506-09.

The conviction in *Morris* blends the idea that access can be controlled and the idea that one who has stored data on a computer has a protected right in those data that extends to the maintenance of the integrity—that is, the existence, current form, and availability—of those data. These are important rights in a society in which important commercial and governmental systems rely on computer processing of information. These rights are also crucial to the establishment of a protected property right in limited distribution information products.

The connection between these criminal and civil laws protecting property rights should be noted. In some states, criminal statutes can be converted directly into civil causes of action.<sup>43</sup> But even in states where this is not possible, the development of criminal law in this area nonetheless reflects a policy of protecting the computer environment, which adds strength to a claim that making information available only in a computer system environment preserves the information holder's right to control access to the data. Thus, rather than saying that the data are directly susceptible to controlled access, the argument here is simply that the owner of the computer system can determine who may enter that protected environment and under what conditions, much as the owner of a house can determine who may visit and when.

### C. Access and Effort to Protect

A right to control access can also be created by the existence of two factors: the information is not generally known, and the person holding the information undertakes efforts to protect it from disclosure to the general public. This property right is most clearly seen in trade secret law. The Uniform Trade Secret Act defines a trade secret as information that derives its value from both not being generally known or readily ascertainable and being the subject of efforts "reasonable under the circumstances to maintain its secrecy."<sup>44</sup> A trade secret is protected against wrongful acts to acquire it in the form of "misappropriation."<sup>45</sup>

There are, then, two elements to protected secrecy: the extent to which the information is generally known and the efforts to protect its secrecy. Determining what satisfies these elements entails an evaluation in light of the practical use and costs of retaining an information product and using the information effectively. "[What] is a 'reasonable' precaution . . . depends on a balancing of costs and benefits . . . . [The] more the owner of the trade secret spends on preventing the secret from leaking out, the more he demonstrates

---

43. See *Safeco Title Insurance Co. v Liberty Natl Title Insurance Co.*, 1989 WestLaw 11079 (ND Ill Feb 9, 1989) (plaintiff allowed to use provisions of previously repealed computer crime statute as basis for civil action).

44. Uniform Trade Secrets Act § 1(4) (1985 approved draft), 14 ULA 438.

45. *Id.*

that the secret has real value . . . . On the other hand, the more he spends, the higher his costs . . . . [P]erfect security is not optimum security.”<sup>46</sup>

To preserve a right to control access to a product under this body of law, the proprietor of the information must create internal safeguards and make disclosures only under conditions that restrict further disclosure by the recipient. While unauthorized access in spite of these practical efforts is not illegal under the trade secrets law, similar violations do exist in other sources of information property law. For example, the Electronic Communications Privacy Act of 1986 (“ECP”) covers data communications in interstate facilities and prohibits unauthorized interception of electronic communications, but it excludes liability for accessing an “electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public.”<sup>47</sup> The 1984 Cable Act proscribes unauthorized reception of cable signals if the signals are scrambled or otherwise protected against reception.<sup>48</sup> By not using protections made possible by existing technology, then, the proprietor loses the right to bar access to the data, effectively committing the material to the public domain.<sup>49</sup>

46. *Rockwell Graphic Systems, Inc. v DEV Industries, Inc.*, 925 F2d 174, 179-80 (7th Cir 1991).

47. 18 USC § 2511(g)(i) (1988). The definition of “intercept” includes acquisition (access) to oral, wire, or electronic communications by electronic, mechanical, or other devices and creates liability where there have been reasonable efforts to restrict access. *Id* § 2510(4).

48. 47 USC § 705 (1988).

49. The Copyright Act permits reception and public display of broadcast signals on apparatus of a kind normally used in homes. 17 USC § 110(5) (1988). In *Home Box Office, Inc. v Corinth Motel, Inc.*, 647 F Supp 1186, 1189-91 (ND Miss 1986), use of a satellite dish to receive cable TV for viewing by hotel guests constituted infringement under § 111(b), which precludes secondary transmission of a primary transmission not originally intended for the public at large. The hotel was not protected by the exemption for public performances on a single receiving apparatus commonly used in private homes because HBO’s transmission could be received only by regular television sets equipped with special equipment not commonly used in a home. The receptions also violated the Federal Communications Act. Compare *National Football League v McBee & Bruno’s, Inc.*, 792 F2d 726 (8th Cir 1986) (restaurants that received NFL football games locally “blacked out” not protected by § 110(5) of the Copyright Act, which applies if the performance received on apparatus commonly used in homes); *International Korwin Corp. v Kowalczyk*, 665 F Supp 652, 657 (ND Ill 1987) (defendant’s receiver was not an ordinary receiving system commonly used in private homes). Section 605(a) of the Federal Communications Act provides in part that:

No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. No person having received any intercepted radio communication, or having become acquainted with . . . such communication . . . knowing that such communication was intercepted, shall divulge . . . such communication . . . .

47 USC § 605(a) (1988). However, § 605(a) does not apply if

- (1) the programming involved is not encrypted; and
- (2)(A) a marketing system is not established under which
  - (i) an agent or agents have been lawfully designated for the purpose of authorizing private viewing by individuals, and
  - (ii) such authorization is available to the individual involved from the appropriate agent or agents . . . .

*Id* § 605(b) (emphasis added). In *Showtime/The Movie Channel, Inc. v Covered Bridge Condominium Assn*, 881 F2d 983, 988-89 (11th Cir 1989), the court held that the private viewer exemption did not apply to a condominium association.

These relationships define both what can be transferred and how a transaction involving limited distribution information must be conducted. The holder's ability to restrict access—its property right—depends in part on the location of the information and in part on maintaining restrictions reasonably designed to preserve the confidential (at least semisecret) nature of the information itself. Contracting in reference to information of this kind must be cast in a form and within limits aimed at protecting and retaining these conditions, on which the property right itself depends.

#### D. Use, Disclosure, and Privacy as Property

In *Eden Hannon & Co. v. Sumitomo Trust & Banking Co.*,<sup>50</sup> the plaintiff was a company that prepared economic information for investors to use in bidding on portfolios of business leases between Xerox and other companies. To attract potential investors, Hannon delivered information to them about the economic models it used before it established an investment contract. Hannon distributed the product (information) under what the court labeled a “non-circumvention” contract, which required that “the investor not disclose the information it receives from [Hannon] to other parties.”<sup>51</sup> The contract also required that the potential investor “not independently pursue lease transactions” with Xerox’s PAS Program for a period of “approximately three years.”<sup>52</sup> The court held this restriction on the use of information and on competing with Hannon to be enforceable:

Often, the value of a firm is its special knowledge, and this knowledge may not be an idea protectible by patent or copyright. If that firm cannot protect that knowledge from immediate dissemination to competitors, it may not be able to reap the benefits from the time and money invested in building that knowledge. If firms are not permitted to construct a reasonable legal mechanism to protect that knowledge, then the incentive to engage in the building of such knowledge will be greatly reduced. Free riders will capture this information at little or no cost and produce a product cheaper than the firm which created the knowledge, because it will not have to carry the costs of creating that knowledge in its pricing. Faced with this free rider problem, this information may not be created, and thus everybody loses.<sup>53</sup>

Hannon’s business was selling expertise and knowledge. If it could not prevent the recipient from competitively misusing the information, the incentive to develop the information and, indeed, the very economic structure of its business would dissipate.

As *Hannon* indicates, it is possible to enforce contractual restrictions on the use or disclosure of information against a third party. In passing on the enforceability of such arrangements, courts rely in part on trade secret law. They also typically review the reasonableness of restraints, essentially asking whether the restriction is related to a valid interest of the person transferring

---

50. 914 F2d 556 (4th Cir 1990), reh’g & reh’g en banc denied.

51. Id at 558.

52. Id.

53. Id at 561.

the data and obtaining consent to the restriction.<sup>54</sup> Indeed, the right to restrict disclosure and use lies at the heart of not only commercializing information distributed on a limited basis, but also retaining a property right when more than one person must know of the information to make it useful.

*Hannon* illustrates that the law distinguishes between possession of information and the right to use it. This distinction can be drawn either by contract or by explicit statutory provision. Statutory restrictions on the use of information commonly govern information held by the government.<sup>55</sup> Insofar as the information relates to individuals, privacy rules, which are a form of property rights law, are implicated. The right stems from the nature of the information and how the product is structured with respect to the data, rather than from how much effort the individual has made to keep the information private. Some personal data are within a protected zone that an individual can control either by resisting disclosure initially or, more commonly, by preventing a person in possession of the data from using and subsequently disclosing the data.

Most reported decisions involving privacy rights that empower the individual to control the use and disclosure of personal information rest on statutory rather than common law authority and involve information held by the government. Computer technology plays a role in defining the types of disclosure that courts have barred. The federal Freedom of Information Act ("FOIA"),<sup>56</sup> for example, exempts information from mandatory disclosure if such disclosure would constitute an unwarranted invasion of privacy. The Supreme Court, in *Department of Justice v. Reporters Committee for Freedom of the Press*,<sup>57</sup> held that the FOIA exemption covered an FBI rap sheet detailing the criminal arrests and convictions of an individual even though the individual items in the FBI database were public information.<sup>58</sup>

The privacy interest in rap sheet information was protected under FOIA, and this did not change because of the "public nature" of the individual records. Nor did the fact that a collateral search might uncover all of the same

---

54. See, for example, *Sunds Defibrator AB v. Beloit Corp.*, 930 F2d 564, 566 (7th Cir 1991) (distinguishing between use and disclosure as elements of control dealt with under a disclosure agreement); *Rockwell Graphic Systems, Inc. v. DEV Industries, Inc.*, 925 F2d 174, 177 (7th Cir 1991) (ability to transfer to third-party support companies and yet retain control is critical factor in using secrets).

55. See, for example, *Ruckelshaus v. Monsanto Co.*, 467 US 986, 1011 (1984) (EPA's disclosure of trade secrets held to frustrate Monsanto's expectations based on the then-current version of FIFRA); *Belth v. Bennett*, 740 P2d 638, 641 (Mont 1987) (corporation can assert a Montana statute that allows for withholding reports from the public as necessary for privacy interests); *Long v. IRS*, 891 F2d 222 (9th Cir 1989) (IRS check sheets exempt from disclosure under the Freedom of Information Act); *Urbaniak v. Newton*, 226 Cal App3d 1128, 1140 (1991) (disclosure of patient's HIV status violated the patient's privacy expectations, in violation of article I § 1 of the California Constitution, which includes privacy among the inalienable rights of citizens).

56. 5 USC § 52 (1988).

57. 489 US 749, 762-71 (1989).

58. Compare *Paul v. Davis*, 424 US 693, 713 (1976) (no privacy violation in the distribution of a list of "active shoplifters" by a state agency; Court relied on the fact that there was a state interest in deterring shoplifting and the fact that arrest records were public information). See also *Whalen v. Roe*, 429 US 589, 600-01 (1977) (no privacy violation in the creation of a drug data bank).

information from state and local sources undermine the individual's interest in withholding disclosure of the compiled summary. The centralized compilation of data in computerized form presents a different privacy risk than does their diffusion among several police agencies.<sup>59</sup> FOIA and similar state laws adumbrate an emerging principle that an individual owns some rights in information about himself if the information is personally sensitive, if it is private, and if it is to be used or disclosed in a form related specifically to the individual.<sup>60</sup>

Most privacy restrictions on disclosure or use of individual data are premised on governmental action, but attempted application of such restrictions to individual data held in private systems is likely to become more frequent in the future. In private sector data, however, the outcome is more uncertain, since there is a presumption that the entity holding data may use it. Indeed, common law privacy lawsuits seldom succeed in preventing or imposing liability for the disclosure of properly collected information unless there is a statutory basis for such action or the disclosure entails fraud or factual error.<sup>61</sup>

There have been some legislative departures from this laissez-faire position in the United States,<sup>62</sup> but the law on data privacy as property has

---

59. This approach to privacy is reminiscent of the closely related area of trade secret law. In that context it is accepted that a combination of facts or methods otherwise in the public domain can be a trade secret as to the combination itself. See, for example, *Integrated Cash Management Services, Inc. v Digital Transactions, Inc.*, 920 F2d 171, 174 (2d Cir 1990).

60. See *Doe v Borough of Barrington*, 729 F Supp 376, 385 (D NJ 1990) (police officer who disclosed AIDS virus infection to third parties violated the infected person's privacy rights). See also *Aronson v IRS*, 767 F Supp 378, 388 (D Mass 1991) ("While access to Social Security numbers would likely assist in locating individuals due refunds, it would do so precisely because it would provide linkage to the vast amount of personal information already in data banks. The serious threat to privacy posed by such easily accessible computerized data banks is well recognized . . . . Because of the capacity of this information to unlock a wide variety of private data and the potential for abuse, public disclosure by the IRS of an individual's Social Security number would not be warranted in this context." (citations omitted)); *Oliva v U.S.*, 756 F Supp 105, 107 (ED NY 1991) (disclosure of social security numbers and birth dates would be "unwarranted invasion of privacy").

61. See, for example, *Minnesota Medical Assn v State*, 274 NW2d 84, 88-89 (Minn 1978) (no statutory basis to prevent Department of Public Welfare from revealing names of medical assistant patients who had abortions); *State ex rel Stephen v Harder*, 641 P2d 366, 375 (Kan 1982) (common law restrictions on public access to abortion records do not apply under the state's public records statute); *Tobin v Michigan Civil Service Comm'n*, 331 NW2d 184, 190 (Mich 1982) (disclosure of names and addresses of employees not invasion of privacy; names and addresses not ordinarily personal or embarrassing facts); *Peninsula Counseling Center v Rahm*, 719 P2d 926, 929-30 (Wash 1986) (en banc) (data disclosed to state about name and diagnosis of patients receiving government funds in subsidized mental health facilities serves interest in ensuring delivery of service to proper parties).

62. See Communications Privacy Act, 18 USC § 2702 (1988) (prohibits persons operating an electronic communication service or providing remote computing services from knowingly divulging the contents of a communication if not authorized by agreement to access the contents); Cable Communications Policy Act, 47 USC § 551 (b-c) (1988) (cable system operator may not use the system to collect personal, identifiable information regarding subscribers without their prior consent except as necessary to operate the cable system; a cable operator can disclose personal information only with the subscriber's consent, a court order, or in connection with its ordinary business); Fair Credit Reporting Act, 15 USC § 1681 (1988) (limits under which credit reports may be issued by reporting agencies); Right to Financial Privacy Act, 12 USC §§ 3401-3422 (1988) (prior notification and other procedures for the disclosure of financial information by a depository institution); Electronic Fund Transfers, 15 USC § 1693c(a)(9) (1988) (electronic fund transfer service contracts

been developed more extensively in Europe, where most countries restrict the disclosure of personal information and its transfer across national borders.

Control of personal data in private hands is significant for both information property law and the commercialization of information. The right to control use of private data will tend to define the products that one can offer and the authorizations required. The existence of a privacy right limits the extent to which any company can use information merely because it holds that information, absent permission of the persons to whom the information relates. For example, a major credit card company recently announced that it was offering a commercial product containing marketing reports and mailing lists derived from data about customers. In addition to the practical restraints on the company's ability to reveal this information, the individuals to whom the data relate can validly claim an ownership right in these data and prevent or control their disclosure to third parties. As seen in *Reporters Committee*,<sup>63</sup> the mere fact that third parties could independently obtain the data from various records in diverse files does not support a right to distribute a report compiling and summarizing personal transactions. The same can be said about merchants' trade secret claims. Who owns the information, and who has a right to commercialize it? Physical possession does not create unfettered ownership rights.

### III

#### QUALITY ASSURANCE

While property law issues define what can be transferred in an information product transaction, an entirely different body of law defines what assurances of quality travel along with the contractual transfer of information. A tempting analogy can be drawn in this regard to the law governing tangible personal property, which deals with issues of both title (that is, ownership) and quality (that is, warranties). Qualitative assurances in information contracts, however, bear little resemblance to warranties of quality in traditional sales of goods. In information transfers, the primary qualitative concerns are whether the information is correct, whether it is relevant to the use for which it was intended, and whether it is delivered in a form that is understandable and, therefore, usable by the recipient.

Unlike transactions involving goods, transactions involving information products do not typically give rise to liability without fault, but rather require at least negligence, if not wrongful intent. Although in sales of goods a promise is implied (unless expressly negated) to deliver goods of acceptable quality, no such promise is recognized as to the accuracy of information sold unless expressly made or unless the information constitutes a warranty concerning goods being sold. In a pure information product, qualitative

---

with consumers establishing funds services must include the circumstances under which the financial institution will disclose information about the consumers); Family Educational Rights Act, 20 USC § 1232(g) (1988) (restricts disclosure of education files).

63. *United States Dept of Justice v Reporters Committee for the Freedom of the Press*, 489 US 749 (1989).

assurances are generally subsumed under the concepts of fraud and negligence, pursuant to which the vendor is not held to any undertaking that the information is correct. Instead, he is penalized only for inaccuracies that are the result of culpable misconduct.

#### A. Quality and Publishers

In the mid-1980s, G. P. Putnam and Sons published a book entitled *The Encyclopedia of Mushrooms*. Relying on information in the book, a family collected, prepared, and ate wild mushrooms. They became violently ill, required liver transplants, and subsequently sued the publisher. Were the publisher and author of the encyclopedia responsible for the injury? In *Winter v. G. P. Putnam's Sons*,<sup>64</sup> the Ninth Circuit held that the publisher was not accountable. Unlike the manufacturer of an automobile or a television set, the publisher of the encyclopedia had no duty to investigate the accuracy of its publications and gave no assurances to buyers that the information published in the book was of a quality on which the buyer could rely.

*Winter* conveys various messages regarding the difference in law between information products and more conventional products sold in the modern marketplace. The *Winter* court refused to apply a product liability standard to a publication about mushrooms.<sup>65</sup> With respect to ordinary goods, society is willing to restrain innovation in order to protect consumers, but refuses to accept a similar limitation with respect to information products. "We accept [instead] the risk that words and ideas have wings we cannot clip and which carry them we know not where. The threat of liability without fault . . . could seriously inhibit those who wish to share thoughts and theories."<sup>66</sup> The court refused to impose any duty on the publisher to investigate the accuracy of the books it published.

Qualitatively speaking, then, only transactions involving negligently or intentionally misleading information can be analogized to those involving defective products of the more conventional kind. This distinction has broken down only in cases involving aeronautical charts that erroneously described altitudes and other critical flight data,<sup>67</sup> which, like other technically detailed and focused distribution products, have exposed their publishers to product liability and negligence claims.

#### B. Quality of Information and Libel

The general policy protecting the publisher of data against the risk of liability for merely negligent error is most often discussed with reference to

---

64. 938 F2d 1033 (9th Cir 1991).

65. Id at 1036.

66. Id at 1035. See also *Walter v Bauer*, 439 NYS2d 821, 822 (S Ct 1981) (publisher was not strictly liable for child's injury in doing a science project described in its book).

67. See, for example, *Brockelsby v United States*, 767 F2d 1288, 1296 (9th Cir 1985) (court applied the Restatement to establish liability); *Saloomey v Jeppesen & Co.*, 707 F2d 671 (2d Cir 1983); *Aetna Casualty & Surety Co. v Jeppesen & Co.*, 642 F2d 339 (9th Cir 1981).

constitutional restraints on the scope of libel and slander law. In enforcing such laws, the state's interest lies in protecting the reputation and public standing of individuals against the publication of false and damaging information rather than in preventing mistaken reliance on erroneous data. Beginning with the landmark Supreme Court decision in *New York Times Co. v. Sullivan*,<sup>68</sup> however, the Court has interposed constitutional barriers against the broad use of state law to protect reputation interests in favor of encouraging authors and commentators to discuss viewpoints, public figures, and issues with lessened risk of liability.

*New York Times* essentially allows one to publish false information about public figures and issues, free of risk of any civil liability, unless such statements are made maliciously or with misleading intent. In *Masson v. New Yorker Magazine, Inc.*,<sup>69</sup> the Supreme Court held that the magazine's use of incorrect quotation marks to attribute certain comments to a public figure could not support a claim of defamation unless the plaintiff could ascribe the use of the incorrect quotation to malice:

We conclude that a deliberate alteration of the words uttered by a plaintiff does not equate with knowledge of falsity . . . unless the alteration results in a material change in the meaning conveyed by the statement. The use of quotations to attribute words not in fact spoken bears in a most important way on that inquiry, but it is not dispositive in every case.<sup>70</sup>

The constitutional bar against liability for nonmalicious defamation of public figures serves to preserve a potentially robust arena for civic debate. This formulation, however, may not apply to information products that deal with material not involving major public issues. In *Dun & Bradstreet v. Greenmoss Builders, Inc.*,<sup>71</sup> for example, the Supreme Court held that constitutional restrictions on liability for defamation did not apply to an information service that wrongly reported that the plaintiff company had filed bankruptcy. Since this report concerned private commercial information and was distributed to a limited subscriber audience, it did not qualify as a protected publication that involved a public figure or issue. Similarly, in *Blue Ridge Bank v. Veribanc, Inc.*,<sup>72</sup> the Fourth Circuit held that inaccurate reports about the financial condition of a bank did not fall within the protected class of publications.

### C. Quality of Information and Fraud

Whether an information product falls within a constitutionally protected zone determines the nature of the standard of liability against which a publisher's conduct is measured rather than whether it is subject to any

---

68. 376 US 254, 279-83 (1964).

69. 111 S Ct 2419 (1991).

70. Id at 2433. Compare *Milkovich v. Lorain Journal Co.*, 110 S Ct 2695, 2707 (1990) (under constitutional standards, claim that statement is merely an opinion is not an absolute defense to libel lawsuit).

71. 472 US 749, 762 (1985).

72. 866 F2d 681, 688-89 (4th Cir 1989).

standard at all. The law of fraud is a dominant force in defining what assurances of quality—that is, accuracy—inhere in information communicated to those who likely will act upon the information. Various statutes creating causes of action grounded in fraud specifically govern published or publicly disclosed information regarding securities and other specially protected areas of trade. Outside of such specially targeted areas, the law of fraud usually applies only to more limited distribution transactions in information. The tort of misrepresentation requires (1) a statement of fact that (2) is inaccurate and (3) leads to detrimental reliance by the party receiving the wrong information.<sup>73</sup> The misrepresentation must, moreover, be made with a requisite mental state—in most states, recklessly, even though the actor need not actually have known of its falsity.<sup>74</sup>

Section 552 of the *Restatement of Torts* defines negligent misrepresentation as a false statement made without exercising reasonable care about the accuracy of the facts asserted.<sup>75</sup> This tort can occur, however, only where information is supplied by a defendant in the business of providing information for the guidance of others. But there still is an unresolved controversy as to whether a claim of negligent misrepresentation will lie where the supplier of false information also engaged in the sale of goods to the buyer who relied on that information.<sup>76</sup>

The tort of fraud and the cases it has generated illuminate an important facet of information as a commodity. The primary quality issue in transactions involving information products is accuracy, which supplants the absence-of-defects criterion that so importantly figures in the case of more conventional goods. Inaccuracy, however, is a much more amorphous concept than is a product defect. Even in limited distribution transactions, there is no general presumption that the information is accurate in an absolute sense. Unless defined in the contract, qualitative assurances—that is, warranties—ordinarily deal only with the information supplier's intent, knowledge, and exercise of care to ensure the accuracy of the information. In cases involving professionals such as doctors and lawyers, of course, reasonable care becomes a malpractice standard.

---

73. See generally William L. Prosser & W. Page Keeton, *The Law of Torts* § 105 (West, 1984).

74. See *Dunn Appraisal Co. v Honeywell Information Sys., Inc.*, 687 F2d 877, 882 (6th Cir 1982); compare *Clements Auto Co. v Service Bureau Corp.*, 444 F2d 169, 176 (8th Cir 1971) ("[I]t is not necessary that the statement is recklessly or carelessly made. It makes no difference how it is made if it is made as an affirmation of which defendant has knowledge, and it is in fact untrue." (citations omitted)).

75. *Restatement (Second) of Torts* § 552 (1977). See, for example, *Computer Sys. Engineering, Inc. v Qantel Corp.*, 740 F2d 59, 67 (1st Cir 1984).

76. See, for example, *Black, Jackson & Simmons Insurance Brokerage, Inc. v IBM*, 440 NE 2d 282 (Ill Ct App 1982) (IBM not liable for negligence; it was in the business of selling merchandise, not supplying information); *Accusystems, Inc. v Honeywell Information Sys., Inc.*, 580 F Supp 474, 481 (SD NY 1984) (same). The issue here involves distinguishing between tort and contract law as a basis for liability in a sale of goods transaction. See *Rio Grande Jewelers Supply, Inc. v Data General Corp.*, 689 P2d 1269, 1270-71 (NM 1984) (negligent misrepresentation claims cannot survive contract disclaimers involving sale of goods).

#### D. Information and Negligence

Some information products entail the delivery of services by processing information *for* third parties. Data-processing and information-management companies may record, compile, and report on management information for their clients. Other companies operate data networks for clients for electronic mail, electronic data interchange, and similar systems.

Regardless of the technology involved, these arrangements are service contracts. The information handler makes a commitment to exercise care in fulfillment of its promised performance. Whether one views this as a warranty or as a quasi-tort duty, it nonetheless entails a negligence rather than an absolute liability standard, and the duty of reasonable care can in most states be disclaimed by contract.<sup>77</sup>

The reasonable care standard is illustrated in *Shell Pipeline Corp. v. Coastal States Trading, Inc.*,<sup>78</sup> in which Shell had undertaken to provide a computerized order-fulfillment system associated with a pipeline system. Shell misdesignated the recipient of the product, resulting in a misdelivery of natural gas and a loss to the supplier. The court held Shell liable for negligently designing a system that failed to identify and prevent the error, for failing to warn the system's users that they might not be able to detect such an error, and for failing to follow its own procedures for verifying or confirming questioned deliveries. "In designing a system that depended upon such an inherently unreliable process as observations of letterheads for distinguishing among various trading companies," the court held that Shell was negligent and hence answerable for the loss caused by misdelivery.<sup>79</sup>

#### CONCLUSION

Information has value. The reciprocal notion that information constitutes commercial property is less widely accepted, however, although this is more important in the information age. Treating information as a commercial subject forces consideration of the constituent elements of property rights in information products and the assurances of quality that inhere in those products.

This article has explored some of the dimensions of information as a valuable subject of commercial transactions. The issues that arise in information transactions differ markedly from conventional product transactions. We need to redefine ideas of property, transfer, and quality in

---

77. See, for example, *Southwestern Bell Telephone Co. v. FDP Corp.*, 811 SW2d 572, 576-77 (Tex 1991) (upholding limitation on liability in yellow pages contract for errors in advertising); *Southwestern Bell Telephone Co. v. Delaney*, 809 SW2d 493, 495 (Tex 1991) (duty to publish advertisement arises solely from contract); *Liberty Financial Management Corp. v. Beneficial Data Processing Corp.*, 670 SW2d 40, 48 (Mo Ct App 1984) (upholding contractual exoneration from liability for ordinary negligence).

78. 788 SW2d 837 (Tex Ct App 1990).

79. *Id.* at 845.

order to understand how to approach this newly expanding subject matter for purposes of commercial trade.

Information as commercial property comprises an intangible interest of potentially great value, but one permeated with constitutional and privacy considerations not present in other commercial products. As we have seen, there is a dichotomy between rights in general access and limited access information products. This distinction, which influences both property rights and liability issues, stems from a fundamental commitment in our society to an open marketplace of ideas, which requires a steady and unhindered infusion of public information and uninhibited debate. Within this framework, a commercial law of information must be carved out.

This article does not purport to resolve the issues that relate to the emergence of information as a commodity, but rather to provide a framework for understanding the structure of the marketplace in which it is traded and the law that governs it. The discussion of these matters will continue into the foreseeable future and will play a vital role in determining the contours of the next century's social and legal system. The time to begin this discussion is today.